**ASSEMBLY PARTE 2**

La figura seguente mostra un estratto del codice di un malware. Identificare i costrutti noti visti durante la lezione teorica

A computer screen shot of a program

Description automatically generated

**Individuazione dei costrutti**

**IF-ELSE**, Questo costrutto verifica se il valore della variabile cmp [ebp+var\_4] è uguale a zero. Se lo è, il programma esegue le istruzioni successive alla locazione 40102B, altrimenti esegue le istruzioni successive alla locazione 401015.

Il costrutto IF-ELSE consente di eseguire un'azione se una condizione è soddisfatta e un'altra azione se la condizione non è soddisfatta.

Viene inoltre utilizzato per verificare se il computer è connesso a Internet. Se lo è, il programma stampa il messaggio "Success: Internet Connection\n". Altrimenti non fa nulla.

**Spiegazione codice**

Creazione dello stack:

nelle prime due righepush ebp e mov ebp, esp avviene la creazione dello stack, il registro ebp viene spostato nello stack poi viene copiato esp in ebp, successivamente ci sono tre push vanno a spostare i valori all’interno dello stack, call va a richiamarsi i tre precedenti valori importati col push e avvia la funzione InternetGetConnectedState (che funzionerà tramite il nostro if)

Costrutto IF-ELSE:

1. Il processore esegue l'istruzione cmp [ebp+var\_4], 0. Questa istruzione confronta il valore della variabile [ebp+var\_4] con zero.
2. Se il valore della variabile [ebp+var\_4] è uguale a zero, il processore esegue l'istruzione jz short loc 40102B. Questa istruzione salta alla locazione 40102B se il valore della variabile [ebp+var\_4] è uguale a zero.
3. Se il valore della variabile [ebp+var\_4] è diverso da zero, il processore esegue le istruzioni successive alla label loc 401015.